Security and Company Culture

By Michael G. McCourt

This article first appeared in the December 2001 issue of Workplace Violence Prevention Reporter*, a national monthly newsletter available in print and electronic versions to subscribers. It is reprinted with permission from Specialty Technical Publishers (www.stpub.com).*

The tragic events of September 11 and subsequent anthrax attacks forever changed the landscape of security in our country.

Before September 11, we thought of ourselves as invincible. Now, we recognize our vulnerability. Our nation has scrambled to create an Office of Homeland Security, called upon our National Guard to provide support, increased the visibility and budgets of law enforcement agencies across the country and devoted resources to developing medical remedies for diseases thought to be extinct.

Corporations, too, have joined the race to develop disaster plans, increase security technology, add security personnel, develop policies and rethink their allocation of resources. These "quick fix" strategies have cost billions of dollars. Despite the phenomenal increase in the cost of safety and security, industry reports say the general public (and employees in particular) does not feel any safer. Why hasn't the increase translated into a greater sense of security?

The answer, simple as it is, has been overlooked for decades in all but the largest of corporations. In order for security to be successful, it has to be a cost-effective function that is woven into the fabric or culture of the corporation.

The first element, cost, is easily defined but challenging nonetheless. Companies allocate financial resources based on return-on-investment (ROI). A declining economy prior to September 11, along with the catastrophic events of that day, has focused more attention than usual on ROI issues.

ROI utilizes a set of varying metrics to measure success. The measure of success in security is "nothingness." (Nothing happened yesterday, nothing is happening today and, hopefully, nothing will happen tomorrow.) Corporate leaders do not as easily embrace this "nothingness" concept, widely accepted by security professionals. It is critically important for senior management to become more aware of, and comfortable with, this metric.

To be effective, security requires a budget equal to, or slightly greater than, the level of threat faced by the organization. Depending on the industry, that number can be significant. Companies have to resign themselves to the fact that security comes at a price. Negligent security, however, comes at a much higher price.

Research indicates that the average out-of-court settlement for a negligent security case is in excess of $500,000, with the average jury award exceeding $1.5 million. The insurance axiom, "it's not a question of whether you can afford it, it's a question of whether you can afford not to have it," applies to security as well.

At a time when the future is less predictable than ever before, the question of whether or not an organization can afford security should be a nonnegotiable, easy answer. Corporations will spend significant amounts of money on programs and technology viewed as being intrinsically tied to the bottom line. Until the time comes when security is viewed in the same regard, companies will continue to expose themselves to risk by providing substandard security programs. However, money alone is not the answer.

Dollars aside, the real challenge for organizations is to integrate security and corporate culture. To marry the two effectively, leadership must be able to define their organizational culture in concrete terms - not by reciting a mission statement or a pie-in-the-sky list of attributes, which may or may not be practiced on a daily basis. Although culture includes many of those elements, it tends to be more oblique and far-reaching in its impact on daily operations.

Every organization has a culture, whether or not it is purposefully defined. Culture is the glue, or set of unspoken guidelines, that dictates employee behavior, guides the decision-making process, influences discipline, supports (or fails to support) customer service and, ultimately, impacts the organization's productivity and profitability. It's not found in any corporate document and is rarely discussed in boardrooms, but its impact is felt in every interaction, at every level of the organization, every day.

What, then, determines corporate culture? Generally, the CEO and the senior staff of an organization define culture. It is based on their personal beliefs, behaviors, operating standards and core ethics. If personal safety, respectful and open communication, honesty in reporting and a belief that every person has value and contributes to the success of the organization are among the leadership's core values, then safety and security may flourish. If, on the other hand, the values listed above are not seen as critical to the success of the organization, then safety and security will take a back seat to programs more directly related to the technical and operational side of the business.

Organizations that have successfully woven safety and security into their culture will factor security into every project, every decision and every action at every level of the organization. Without the support of senior management, security is doomed to become a part-time program, subject to the "issue of the month" methodology of management.

What can an organization do to integrate security into its culture? Adopt the following strategies:

- Create the position of Chief Safety Officer (CSO) and grant that individual access to the board of directors.

- Ensure that individuals assigned responsibility for security will receive adequate training.
- Make security an agenda item at every board or senior staff meeting.
- Include articles on safety and security in corporate newsletters.
- Develop reward incentives for employees reporting safety and security breaches.
- Sponsor safety and security-related programs within your community.
- Develop disaster plans capable of addressing today's unique environment.

- Post signs and information relating to safety and security throughout the organization.
- Develop policies addressing safety and security, and enforce them fairly and consistently.

Often, solid security strategies will be objected to on the premise that they will cost too much money. Ironically (as these points demonstrate), successful security costs more time than money.

The time to integrate security into corporate culture is now. Corporate leaders have a choice to make - they can continue to underestimate the importance of security and pay the price down the line, or they can make a conscious decision to incorporate security into their culture and defend their human resources, capital investments and intellectual properties against the challenges we face in the 21st century.

Michael G. McCourt is the president and founder of Michael G. McCourt Associates, Inc., a Massachusetts-based consulting firm specializing in workplace violence prevention and counseling. He may be reached at (508) 833-7171 or by e-mail at mgmassoc@adelphia.net.